SANS SECURITY AWARENESS

Drošības izpratnes ieviešanas ceļvedis – drošs darbs no mājām

Kopsavilkums

Koronavīrusa dēļ daudzas organizācijas nonāk situācijā, kad darbaspēks pāriet uz darbu no mājām. Tas var radīt izaicinājumu, jo daudzām organizācijām nav atbilstošas politikas, tehnoloģiju un apmācības, lai nodrošinātu, ka darbaspēks var strādāt attālinātā darba režīmā. Turklāt daudziem darbiniekiem doma par darbu no mājām var šķist sveša vai netīkama. Šī ceļveža mērķis ir palīdzēt jums ātri apmācīt šos cilvēkus, lai viņu darbs būtu pēc iespējas drošāks. Ja jums ir radušies jautājumi par šī ceļveža izmantošanu, sazinieties ar mums pa e-pastu support@sans.org.

Tā kā jūsu darbaspēks, visticamāk, piedzīvo lielu stresu un pārmaiņas un jūsu organizācijas rīcībā visdrīzāk ir ierobežots laiks un resursi, šī stratēģiskā ceļveža mērķis ir padarīt minēto apmācību pēc iespējas vienkāršāku. Mēs iesakām jums koncentrēties tikai uz vissvarīgākajiem riskiem ar vislielāko ietekmi, kuri ir aprakstīti tālāk. Uztveriet šo aprakstu kā sākumpunktu. Ja vēlaties papildināt to ar vēl citu informāciju par riskiem vai tēmām, nevilcinieties to darīt. Vienkārši apzinieties, ka, jo vairāk darbību, procesu vai tehnoloģiju pieprasīsiet jūsu darbaspēkam izmantot, jo mazāka ir iespēja, ka viņi varēs to visu nodrošināt.

Kā izmantot šo ceļvedi

Mēs iesakām jums sākt, izlasot šajā ceļvedī iekļauto materiālu un aplūkojot tajā ietvertās saites uz dažādajiem materiāliem, lai sniegtu jums priekšstatu par pieejamajiem resursiem. Jūs pamanīsiet, ka attiecībā uz katru risku mēs nodrošinām dažādus materiālus, kurus varat izmantot, lai iesaistītu un apmācītu jūsu organizācijas personālu. Tas ļauj jums izvēlēties pieejas, kuras, jūsuprāt, visefektīvāk atbildīs jūsu organizācijas vajadzībām un kultūrai. Kad esat pabeidzis lasīt šo dokumentu, izlasiet gan pievienoto komunikācijas veidni, gan faktu lapu, kas iekļautas šajā komplektā, lai labāk izprastu, ko jūs mēģināt sasniegt. Pēc dokumentu izskatīšanas jums jāsaskaņo rīcība ar divām darbinieku grupām.

1. **Drošības komanda**: konsultējieties ar savu drošības komandu, lai gūtu labāku izpratni par galvenajiem riskiem, kurus mēģināt pārvaldīt. Šajā ceļvedī mēs esam norādījuši, mūsuprāt, vislielākos un visizplatītākos riskus situācijā, kad darbaspēks strādā no mājām, taču jūsu riski var būt atšķirīgi. Mēs vēlamies jūs brīdināt, ka izplatīta kļūda, ko pieļauj drošības komandas, ir mēģinājumi pārvaldīt visus riskus un cilvēku apgrūtināšana ar daudzām politikām un prasībām. Centieties pēc iespējas ierobežot novēršamo risku apjomu. Tiklīdz nosakāt šos riskus un to prioritāro nozīmi, apstipriniet darbības šo risku pārvaldībai. Kā minēts iepriekš, ja jūsu organizācijai nav pietiekami daudz laika vai resursu šim nolūkam, lietderīgi izmantojiet dokumentā tālāk sniegto informāciju.

2. **Komunikācijas nodaļa**: tiklīdz nosakāt galvenos riskus cilvēkiem un galvenās darbības šo risku pārvaldībai, sazinieties ar savu Komunikācijas nodaļu, lai iesaistītu jūsu darbiniekus šajās darbībās un apmācītu viņus tajās. Visefektīvāko drošības izpratnes programmu pamatā ir spēcīga partnerība ar komunikācijas komandu. Ja iespējams, pārliecinieties, vai jūs varētu pat iekļaut kādu no komunikācijas komandas darbiniekiem savā drošības komandā. Iepazīstinot savu darbaspēku ar šo apmācību, efektīva pieeja darbinieku piesaistīšanai ir uzsvērt atziņu, ka šī apmācība ne tikai aizsargās viņus darbā, bet arī ļaus viņiem parūpēties par kiberdrošību mājās, tādējādi aizsargājot sevi un savu ģimeni.

Kopumā, strādājot kopā ar šīm divām komandām, jūs mēģināt gan padarīt drošības ievērošanu pēc iespējas vienkāršāku savam darbaspēkam, gan motivēt savu darbaspēku — šie divi galvenie elementi kalpo kā pamats rīcības maiņai. Mēs iesakām pat izveidot konsultatīvo padomi, kas aptver galvenos cilvēkus, kuru atsauksmes un ieguldījums jums ir nepieciešams apmācības programmas ieviešanai. Papildus jūsu drošības un komunikāciju komandai jums vajadzētu sadarboties un saskaņot rīcību arī, piemēram, ar Personāldaļu un Juridisko nodaļu.

MGT433 digitālās lejupielādes pakotne

SANS Institute nodrošina divu dienu apmācības kursu MGT433: kā izveidot, uzturēt un izvērtēt iedarbīgu drošības izpratnes veicināšanas programmu. Šī intensīvā apmācība nodrošina visu nepieciešamo teoriju, praktiskās iemaņas, sistēmu un resursus, lai izveidotu iedarbīgu drošības izpratnes veicināšanas programmu, kas ļauj efektīvi pārvaldīt un izvērtēt jūsu riskus cilvēkiem. Šajā ceļvedī mēs nodrošinām bezmaksas piekļuvi kursa digitālās lejupielādes pakotnei, kas ietver veidnes un plānošanai nepieciešamos resursus. Kaut arī šie materiāli, visticamāk, pārsniedz šīs iniciatīvas vajadzības, tie var būt noderīgi lielākām organizācijām vai sarežģītāka rakstura ieviešanas pasākumiem.

Atbildes uz darbaspēka jautājumiem

Papildus darbinieku informēšanai un viņu apmācībai mēs ļoti iesakām arī ieviest kādu tehnoloģiju vai forumu, kas ļauj jums atbildēt uz cilvēku jautājumiem, vēlams, reāllaikā. Tas var ietvert īpašu e-pasta aizstājvārdu, Skype vai Slack tērzēšanas kanālu vai arī kāda veida tiešsaistes forumu, piemēram, izmantojot Yammer pakalpojumu. Vēl viena laba ideja ir nodrošināt tīmekļa apraidi par drošības jautājumiem, kuru jūs atkārtojat vairākas reizes nedēļā, lai cilvēki varētu izvēlēties sev piemērotāko laiku un apmeklēt notikumu tiešraidē un, iespējams, pat uzdot jautājumus. Tā mērķis ir padarīt drošības informāciju pēc iespējas pieejamāku un palīdzēt cilvēkiem rast atbildes uz viņu jautājumiem. Šī ir fantastiska iespēja piesaistīt sava darbaspēka interesi un padarīt drošības jautājumus mazāk biedējošus, tāpēc mēģiniet to izmantot. Ņemiet vērā: lai tas būtu efektīvi, jums jānodrošina resursi, kas pārraudzīs visus drošības informācijas kanālus un aktīvi atbildēs uz jautājumiem.

Riski un mācību materiāli

Mēs esam noteikuši trīs galvenos riskus, kas jāpārvalda attiecībā uz jūsu darbaspēku attālinātā darba režīmā. Tie kalpo kā sākumpunkts un, visticamāk, būs jums visnozīmīgākie. Pie katra no tālāk aprakstītajiem riskiem ir norādītas saites uz vairākiem resursiem, lai palīdzētu informēt un apmācīt darbiniekus par attiecīgo tēmu. Mēs nodrošinām vairākus komunikācijai nepieciešamos materiālus, lai jūs varētu izvēlēties tos, kuriem būs vislielākā ietekme uz jūsu organizācijas kultūru. Turklāt gandrīz visi materiāli ir sagatavoti vairākās valodās. Ja tas viss jums šķiet par daudz un jūsu laiks ir ārkārtīgi ierobežots, tad iesakām vienkārši izvēlēties un izmantot divus no tālāk norādītajiem materiāliem.

1. Faktu lapa par drošu darbu no mājām (iekļauta jūsu ieviešanas komplektā).
2. Videoklips Mājokļa kiberdrošības stiprināšana (angļu valodā) ir pieejams arī citās valodās šeit

Sociālā inženierija

Viens no lielākajiem riskiem, ar kuru saskaras attālinātā darba režīmā strādājošie, jo īpaši šajos dramatisko pārmaiņu un neatliekamās steidzamības apstākļos, ir sociālās inženierijas uzbrukumi. Sociālā inženierija ir psiholoģisks uzbrukums, kurā uzbrucēji apkrāpj vai apmāna savus upurus, liekot viņiem kļūdīties, kas šajā pārmaiņu un apjukuma laikā kļūst vēl jo vienkāršāk. Ir būtiski apmācīt cilvēkus par to, kas ir sociālā inženierija, kā pamanīt visizplatītākos sociālās inženierijas uzbrukuma rādītājus un kā rīkoties, kad tādi pamanīti. Pārliecinieties, vai koncentrējaties ne tikai uz e-pasta pikšķerēšanas uzbrukumiem, bet arī informējiet par citām metodēm, piemēram, tālruņa zvaniem, īsziņām, sociālajiem plašsaziņas līdzekļiem vai viltus ziņām. Materiālus, kas nepieciešami apmācībai par šo tēmu un zināšanu nostiprināšanai, varat atrast mūsu mapē Sociālās inženierijas atbalsta materiāli. Papildus šeit ir pieejami divi SANS videoklipi par drošības izpratni, uz kuriem varat norādīt saites un kuri arī ir sniegti vairākās valodās.

- Videoklips Sociālā inženierija (angļu valodā) ir pieejams arī citās valodās šeit
- Videoklips Pikšķerēšana (angļu valodā) ir pieejams arī citās valodās šeit

Stipras paroles

Kā tika norādīts ikgadējā Verizon datu pārkāpumu izmeklēšanas ziņojumā (Data Breach Investigations Report, DBIR), vājas paroles joprojām ir viens no galvenajiem pārkāpumu veicinātājiem globālā mērogā. Tālāk ir norādītas četras galvenās darbības, kas palīdz pārvaldīt šo risku. Jūs varat atrast materiālus, kas nepieciešami apmācībai par šo tēmu un zināšanu nostiprināšanai, un informāciju par minētajām četrām galvenajām darbībām mapē Paroles.

- Ieejas frāzes (ņemiet vērā, ka paroļu sarežģītība un paroļu derīguma termiņi vairs nav šķēršļi).

- Unikālā parole ikvienam kontam
- Paroļu pārvaldnieki
- Daudzfaktoru autentifikācija (Multi-Factor Authentication, MFA). Bieži tiek dēvēta arī par divfaktoru autentifikāciju vai divsoļu pārbaudi.

Atjauninātas sistēmas

Trešā riska novēršanas darbība ir nodrošināt, ka jebkurai tehnoloģijai, kuru izmanto jūsu darbaspēks, ir instalētas operētājsistēmas, lietojumprogrammu un mobilo lietotņu jaunākās versijas. Cilvēkiem, kuri izmanto personīgās ierīces, iespējams, būs jāiespējo automātiska atjaunināšana. Materiāli, kas ir nepieciešami apmācībai par šo tēmu un zināšanu nostiprināšanai, ir pieejami mapē Ļaunprogrammatūra vai Mājokļa kiberdrošības stiprināšana.

Papildu tēmas, kas jāņem vērā

- **Wi-Fi**: jūsu Wi-Fi piekļuves punkta aizsardzība. Šī tēma ir aprakstīta tēmas Mājokļa kiberdrošības stiprināšana materiālos. Lūdzu, skatiet arī videoklipu Mājokļa kiberdrošības stiprināšana (angļu valodā), kas pieejams arī citās valodās šeit.

- **VPN**: kas ir VPN un kāpēc jums tas jāizmanto. Mēs iesakām iepazīties ar OUCH! biļetenu par VPN.

- **Drošība, strādājot attāli**: Attiecas uz cilvēkiem, kuri strādā attāli, bet NE no mājām, piemēram, strādā, atrodoties kafejnīcā, lidostas terminālī vai viesnīcā. Apsveriet iespēju izmantot mūsu videoklipu Drošība, strādājot attāli (angļu valodā) , kas pieejams arī citās valodās šeit.

- **Bērni/viesi**: Lai nostiprinātu domu, ka ģimenes locekļiem/viesiem nevajadzētu piekļūt ar darbu saistītām ierīcēm, apsveriet iespēju izmantot mācību videoklipu Drošība, strādājot attālināti (angļu valodā), kas pieejams arī citās valodās šeit.

- **Konstatēšana/reakcija**: Vai vēlaties, lai cilvēki ziņo, ja, viņuprāt, strādājot no mājām, noticis kāds incidents? Ja tā ir, kas un kad viņiem būtu jāziņo? Tas ir aprakstīts mūsu tēmas Uzlaušana materiālos.

OUCH! biļeteni

Turklāt apsveriet iespēju savas programmas atbalstam izmantot publiski pieejamos OUCH! biļetenus, no kuriem katrs ir tulkots vairāk nekā divdesmit valodās. Tālāk ir norādīti OUCH! biļeteni, kas, mūsuprāt, var sniegt vislabāko atbalstu jūsu iniciatīvai "Drošs darbs no mājām". Visi biļeteni ir pieejami tiešsaistes OUCH! drošības izpratnes biļetenu arhīvā.

PĀRSKATS

Four Steps to Staying Secure (Četri soļi, lai paliktu drošībā)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Mājokļa kiberdrošības stiprināšana)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

SOCIĀLĀ INŽENIERIJA

Social Engineering (Sociālā inženierija)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (Ziņojumapmaiņa / smikšķerēšana)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Personalizētas shēmas)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Uzdošanās par vadītāju)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (Uzbrukumi ar tālruņa zvanu / shēmu starpniecību)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Apturiet pikšķerēšanu)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Krāpniecība, izmantojot sociālos tīklus)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

PAROLES

Making Passwords Simple (Vienkārša paroļu lietošana)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (Uzlabojiet pieteikšanās drošību (2FA))
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

PAPILDU

Yes, You Are a Target (Jā, arī jūs esat mērķis)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Mājas viedierīces)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Ātrie padomi

Padomi un viltības vienkārši izmantojamā formātā, ar kurām varat ērti dalīties.

- Visefektīvākās darbības, kuras varat veikt, lai aizsargātu bezvadu tīklu mājās, ir mainīt noklusējuma administratora paroli, iespējot WPA2 šifrēšanu un izmantot spēcīgu bezvadu tīkla paroli.
- Apziniet visas ierīces, kas pievienotas jūsu mājas tīklam, tostarp mazuļu uzraudzības ierīces, spēļu konsoles, televizoru, ierīces vai pat jūsu automašīnu. Pārliecinieties, vai visas šīs ierīces ir aizsargātas ar spēcīgu paroli un/vai tajās darbojas operētājsistēmas jaunākā versija.
- Viens no efektīvākajiem veidiem, kā aizsargāt jūsu datoru mājās, ir pārliecināties, vai gan operētājsistēma, gan jūsu lietojumprogrammas ir ielāpotas un atjauninātas. Aktivizējiet automātisko atjaunināšanu, kad vien iespējams.
- Galu galā vislabākais aizsardzības veids ir jūsu pārdomāta rīcība. Ja e-pasta ziņa, tālruņa zvans vai tiešsaistes ziņojums šķiet savāds, aizdomīgs vai pārāk daudzsološs, tas var būt uzbrukums.
- Pārliecinieties, vai ikvienam jūsu kontam ir atsevišķa unikāla parole. Vai nevarat atcerēties visas savas paroles/ieejas frāzes? Apsveriet iespēju visu savu paroļu pārvaldībai izmantot paroļu pārvaldnieku.
- Divsoļu pārbaude ir viena no labākajām darbībām, ko varat veikt sava konta aizsardzībai. Divsoļu pārbaude nozīmē, ka nepieciešama gan parole, gan kods, kas tiek

nosūtīts uz jūsu mobilo ierīci vai ko ģenerē jūsu mobilā ierīce. Tādu pakalpojumu piemēri, kas atbalsta divsoļu pārbaudi, ir Gmail, Dropbox un Twitter.

- Pikšķerēšana nozīmē, ka uzbrucējs mēģina jūs apmānīt, lai jūs noklikšķinātu uz ļaunprātīgas saites vai atvērtu pielikumu e-pastā. Izturieties ar aizdomām pret jebkuru e-pasta vai tiešsaistes ziņojumu, kas rada steidzamības sajūtu, satur pareizrakstības kļūdas vai sākas ar uzrunu "Cienījamais klient!".

Rādītāji

Šajā situācijā ir grūti noteikt rīcības rādītājus, jo ir grūtāk izvērtēt, kā cilvēki rīkojas mājās. Turklāt daži no šiem rīcības veidiem neattiecas specifiski uz darbu (piemēram, Wi-Fi ierīces aizsardzība). Tomēr jūs varat izvērtēt iesaisti. Esam secinājuši, ka tādas personiskas vai emocionālas tēmas kā šī var būt ļoti saistoša, raisot daudz lielāku interesi nekā citas tēmas. Tādējādi var būt noderīgi tālāk minētie rādītāji.

- **Saskarsme**: cik bieži cilvēki uzdod jautājumus, publicē idejas vai pieprasa palīdzību jebkurā no jūsu nodrošinātajiem drošības informācijas kanāliem vai forumiem?
- **Simulācijas**: veiciet dažu veidu sociālās inženierijas simulācijas, piemēram, uzbrukumus ar pikšķerēšanas, īsziņu vai tālruņa zvanu starpniecību.

Lai iegūtu daudz pilnīgāku rādītāju sarakstu, lejupielādējiet interaktīvo drošības izpratnes rādītāju matricu no MGT433 digitālās lejupielādes pakotnes.

Licence

Ieviešanas komplekta autors

Lansam Špicneram (Lance Spitzner) ir vairāk nekā 20 gadu drošības pieredze kiberdraudu izpētes, drošības arhitektūras, kā arī izpratnes veicināšanas un apmācības jomās. Viņš veicināja revolucionāru attīstību maldināšanas novēršanas un kiberinteliģences jomās, izveidojot pievilināšanas tīklus (honeynet) un nodibinot organizāciju Honeynet Project. Kā SANS instruktors viņš izstrādāja MGT433: drošības izpratne un MGT521: drošības kultūra. Turklāt Lanss ir publicējis trīs grāmatas par drošību, sniedzis konsultācijas vairāk nekā 25 valstīs un palīdzējis vairāk nekā 350 organizācijām izveidot drošības izpratnes un kultūras programmas, lai pārvaldītu to risku cilvēkiem. Lanss bieži vada raidījumus, regulāri tvīto (@lspitzner) un strādā pie daudziem sabiedrības drošības projektiem. Pirms darba informācijas drošības nozarē L. Špicners bija armijas ātrās reaģēšanas vienības bruņutanku divīzijas virsnieks un ieguva maģistra grādu Ilinoisas Universitātē.

Par SANS Institute

SANS Institute tika nodibināts 1989. gadā kā pētniecības sadarbības un izglītības organizācija. SANS ir visuzticamākais un līdz šim lielākais kiberdrošības apmācības un sertifikācijas pakalpojumu sniedzējs valdību un komerciestāžu speciālistiem visā pasaulē. Atzīti SANS pasniedzēji māca vairāk nekā 60 dažādus kursus, nodrošinot vairāk nekā 200 tiešraides kiberdrošības apmācības pasākumus, kā arī apmācības tiešsaistē. SANS Institute saistītais uzņēmums GIAC apstiprina speciālistu kvalifikācijas, izmantojot vairāk nekā 35 praktiskus, tehniskus kiberdrošības sertifikātus. Reģionāli akreditēts neatkarīgs meitasuzņēmums SANS Technology Institute piedāvā maģistra grādus kiberdrošībā. SANS nodrošina InfoSec kopienai plašu bezmaksas resursu klāstu, tostarp vienprātības projektus, pētījumu ziņojumus un biļetenus, un tas nodrošina arī interneta agrīnās brīdināšanas sistēmu Internet Storm Center. SANS darbības pamatā ir daudzie drošības speciālisti, kuri pārstāv dažādas pasaules organizācijas, sākot no korporācijām un beidzot ar universitātēm, un sadarbojas, lai palīdzētu visai informācijas drošības kopienai. (https://www.sans.org)